SonicWALL Email Security Solutions

EMAIL SECURITY | **SonicWALL Email Security**

SonicWALL Email Security 8000 Getting Started Guide

SONICWALL®

SonicWALL Email Security 8000
Getting Started Guide

This *Getting Started Guide* contains installation procedures and configuration guidelines for deploying a SonicWALL Email Security appliance on your network.

SonicWALL Email Security provides effective, high-performance and easy-to-use inbound and outbound email threat protection. Ideal for the small to medium size business, this self-running, self-updating appliance delivers powerful protection against spam, virus and phishing attacks in addition to preventing leaks of confidential information. Combining anti-spam, anti-phishing, content filtering, policy management and content compliance capabilities in a single seamlessly integrated solution, SonicWALL Email Security provides powerful protection without complexity.

Note: *SonicWALL TotalSecure Email provides complete protection from spam, virus attacks and phishing. Without TotalSecure Email, to use the spam and phishing protection provided by the SonicWALL Email Security appliance, you must have a subscription to SonicWALL Email Protection and Dynamic Support. If you need to purchase a subscription, contact your SonicWALL vendor.*

Please read this entire Getting Started Guide before setting up your SonicWALL Email Security 8000 appliance, and note that an updated version of this guide may exist. Refer to SonicWALL's Documentation Web site for complete, updated documentation at:<http://www.sonicwall.com/Support.html>.

Contents

This document contains the following sections:

1 Before You Begin

Check Package Contents

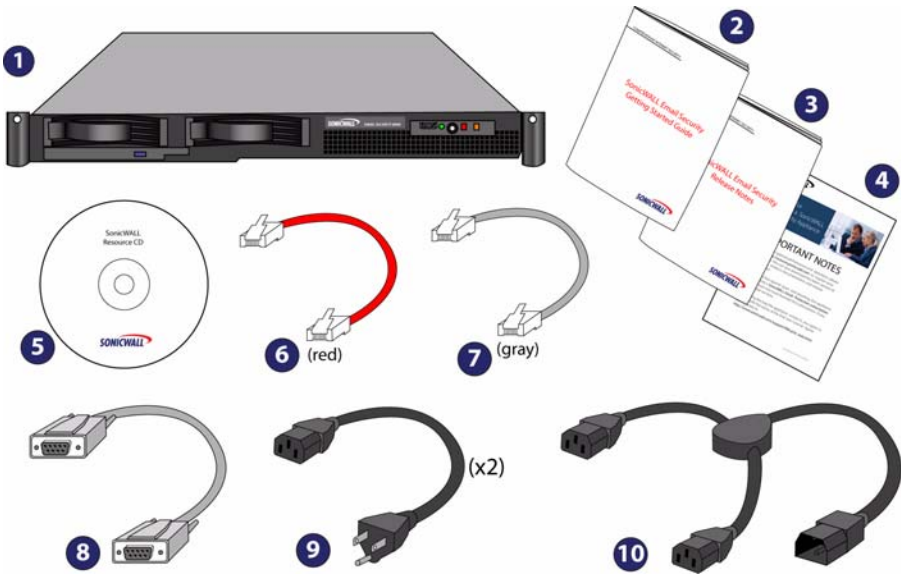
1. One SonicWALL Email Security appliance
2. One Getting Started Guide document
3. One Release Note document
4. One Thank You card
5. One SonicWALL Resource CD
6. One crossover cable (red)
7. One Ethernet cable (gray)
8. One RS232 CLI cable
9. Two standard power cords*
10. One Y-Split power cable*
11. One Rack mount Kit (not pictured)

Any Items Missing?

If any items are missing from your package, contact:
SonicWALL Support
<http://www.sonicwall.com/us/Support.html>
Email: customer_service@sonicwall.com

* *The included power cords are intended for use in North America only. For European Union (EU) customers, power cords are not included.*

* *Das eingeschlossene Netzkabel ist für Gebrauch in Nordamerikas nur vorgehabt. Für Europaïsche Union (EU) Kunden, ist ein Netzkabel nicht eingeschlossen.*



What You Need to Begin

- A computer to use as a management station for initial configuration of SonicWALL Email Security software
- Internet Explorer 5.0 or higher
- An Internet connection

Record Configuration Information

Before continuing, record the following configuration information for your reference:

Registration Information

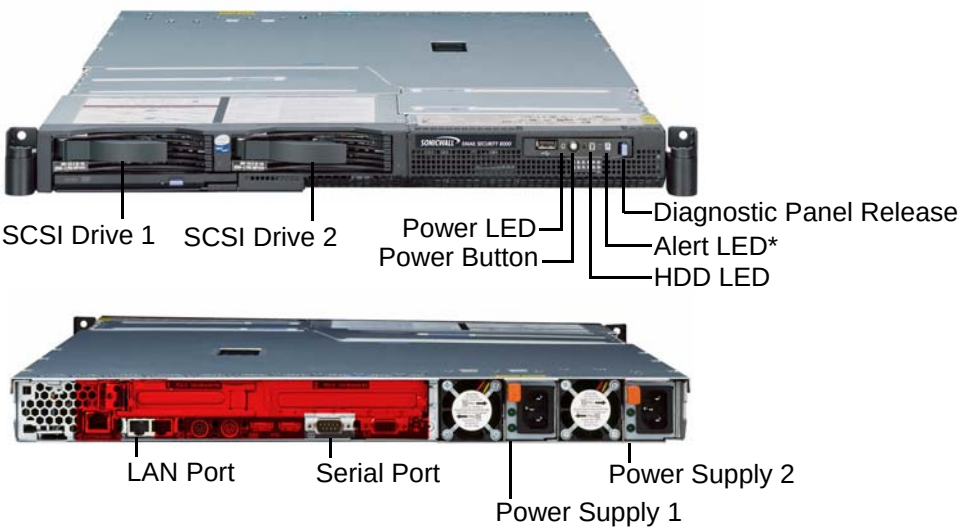
Serial Number: _____ (xxxxxx-xxxxxx)	Record the serial number found on the top right access panel of your SonicWALL Email Security appliance.
Authentication Code: _____ (xxx-xxx)	Record the authentication code found on the top right access panel of your SonicWALL Email Security appliance.

Networking Information

Email Security IP Address: _____	Select a free static IP address for your SonicWALL Email Security appliance that is within the range of your local subnet.
Email Security Subnet Mask: _____	Enter the subnet mask for the local subnet where you are installing your SonicWALL Email Security appliance.
Gateway IP Address: _____	Record the IP address of your network's gateway device (such as your perimeter firewall/router).
DNS Server 1: _____ **DNS Server 2** (optional): _____	Record your DNS Server information.
Host Name: _____	Record the fully qualified domain name within your network for your SonicWALL Email Security appliance (maximum 32 characters).
Password: _____	Select a password for your SonicWALL Email Security appliance (default is *password*).
Email Server IP: _____	Record the IP address or hostname of your email server.
LDAP Server IP: _____	Record the IP address or hostname of your directory services server, such as LDAP or Microsoft Active Directory.

Overview of the SonicWALL Email Security Appliance

SonicWALL Email Security Appliance



* Alerts are explained in detail in light path diagnostic panel. To access, push the diagnostic panel release latch to the left and pull out the panel.

Alert: *Do not plug devices into any ports (other than those indicated) unless explicitly instructed to do so by a SonicWALL technical support representative. Doing so may void your warranty.*

SCSI Drive Bays	Allows SCSI drives in a RAID array to be hot-swapped should one drive fail.
Power LED	Indicates the SonicWALL Email Security appliance is powered on.
Power Button	Allows the SonicWALL Email Security appliance to power on or off.
Diagnostic Panel	Can be pulled out (push release lever to the left) for detailed explanation of alerts.
Alert LED	Indicates an alert. See Diagnostic panel for more information.
HDD LED	Indicates data transfer to and from the hard disk drive.
LAN Port	Allows the SonicWALL Email Security appliance to connect to your local area network or management station.
Serial Port	Allows direct connection to the appliance via terminal services to use the CLI.
Power Supplies	Two power supplies allow the SonicWALL Email Security appliance to utilize redundant AC power using the supplied power cables.

2 Registering Your SonicWALL Email Security Appliance

Before you can use your SonicWALL Email Security appliance, you must first register your appliance and activate your licenses for the SonicWALL Email Protection Subscription and Dynamic Support.

This section contains the following sub-sections:

Before You Register

You need a mysonicwall.com account to register the SonicWALL Email Security appliance. To create a mysonicwall.com account, refer to "Creating a mysonicwall.com Account" on page 8. If you already have a mysonicwall.com account, go to "Registering Your SonicWALL Email Security Appliance" on page 9 to register your appliance.

Note: *mysonicwall.com registration information is not sold or shared with any other company.*

Creating a mysonicwall.com Account

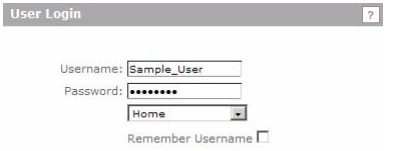
Creating a mysonicwall.com account is fast, simple, and FREE. Simply complete an online registration form.

1. In your Web browser, go to <https://www.mysonicwall.com/>.
2. In the User Login section, click **If you are not a registered user, Click here.**

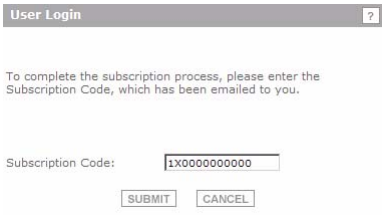
3. Enter the account information, personal information, and preferences and click **Submit**.

Note: *You must enter a valid email address.*

4. Follow the prompts to finish creating your account. SonicWALL will email a subscription code to the email address you entered in the personal information.
5. When you return to the login screen, log in with your new **username** and **password**.



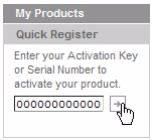
6. Confirm your account by entering the **subscription code** you received in the email.



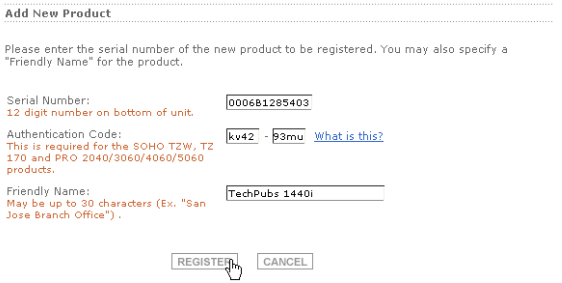
Congratulations! You have created and logged into your mysonicwall.com account.

Registering Your SonicWALL Email Security Appliance

1. Locate your SonicWALL Email Security Software serial number. It should be printed on the label on the top right access panel of your SonicWALL Email Security appliance.
2. If you are not already logged into mysonicwall.com, go to <https://www.mysonicwall.com/> and log in.
3. Enter your serial number in the **Quick Register** field and click the small gray arrow. Follow the on-screen instructions.



4. Confirm your serial number, enter a friendly name for your appliance, and enter your authentication code in the **Quick Register > Add New Product** section.



5. Click REGISTER.
6. Follow the online prompts to fill out the survey and complete the registration process.

3 Initial Setup and Configuration

This section contains the following sub-sections:

Apply Power to the SonicWALL Email Security Appliance

1. Connect the included standard power cord with the y-split power cord.
2. Plug each of the y-split ends into a power supply on the back of the SonicWALL Email Security appliance.
3. Plug the power cord into an appropriate power outlet.
4. Press the recessed power button on the front bezel to power on the appliance. The entire sequence may take several minutes to complete.

Note: *The Power LED on the front panel lights up green when you power on the SonicWALL Email Security appliance. The HDD LED lights up and may blink while the appliance performs a series of diagnostic tests. When the HDD LED is no longer lit, the SonicWALL Email Security appliance is ready for configuration.*

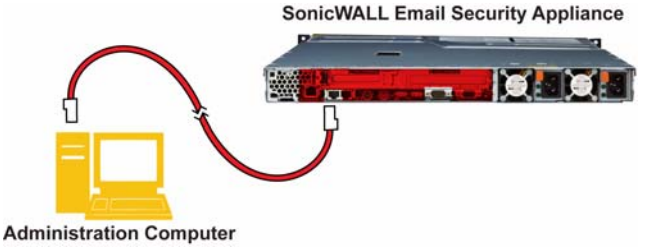
Note: *If the Alert light stays lit, ensure that BOTH of the power supplies on the back of the SonicWALL Email Security Appliance are plugged in (use the included y-split cable for this purpose).*

Connect Directly to the SonicWALL Email Security Appliance

The SonicWALL Email Security appliance comes configured with an IP address of **192.168.168.169**. **Before you can connect your management station to it, you must configure your management station to have an address in the same subnet.**

1. Make a note of your computer's current network settings.
2. Set the computer you use to manage the SonicWALL Email Security appliance to have a static IP address in the 192.168.168.x range, such as **192.168.168.50** and a netmask of **255.255.255.0**. For help with setting up a static IP address on your computer, refer to "Troubleshooting" on page 27.

3. Using the supplied crossover cable and the computer you are using to administer the SonicWALL Email Security appliance, connect the LAN port on the computer to the **LAN (1)** port on the back of your SonicWALL Email Security appliance.



Login to the SonicWALL Email Security Appliance

1. Open a Web browser on the computer you are using to administer the SonicWALL Email Security appliance.
2. Enter **http://192.168.168.169** (the default IP address of the SonicWALL Email Security appliance) in the **Location** or **Address** bar. The SonicWALL Email Security Web management login screen displays.

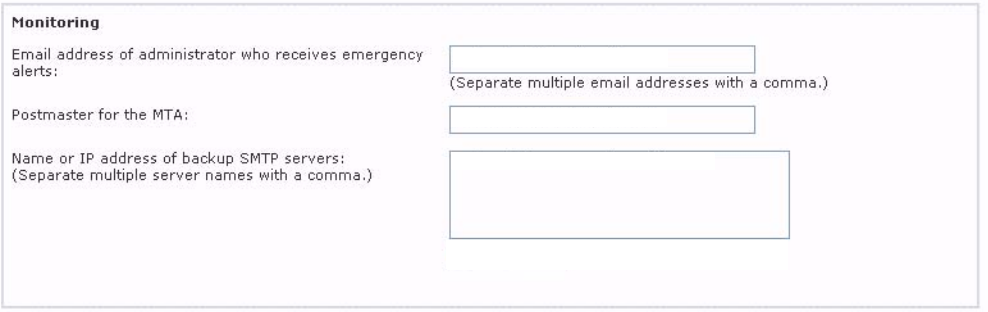
Note: *Depending on your browser settings, **one or more** security warnings may display while connecting to the Email Security Web management interface. Choose to accept the certificates in order to log into the SonicWALL Email Security appliance.*

3. Log into SonicWALL Email Security appliance using "**admin**" as the user name and "**password**" as the password.

Initial System Configuration

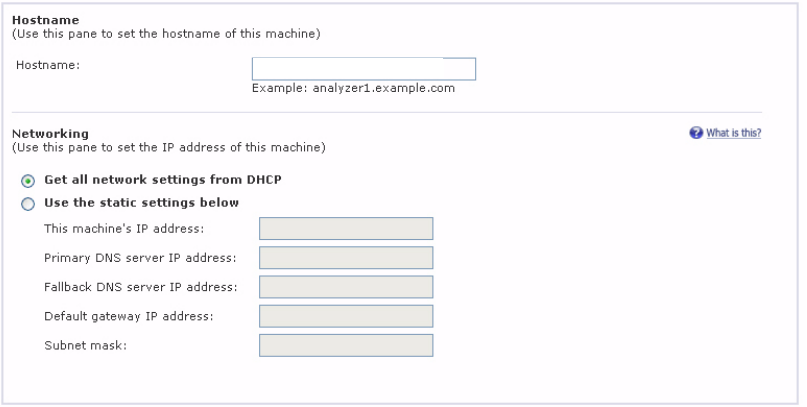
1. The first time you log in to the SonicWALL Email Security appliance, you are directed to the system configuration page. Configure your settings as follows:

Monitoring



Email address of the administrator who receives emergency alerts:	The email address of the mail server administrator. Enter the complete email address. For example, *user@example.com*
Postmaster for the MTA:	The email address of the Mail Transfer Agent administrator who will receive non-deliverable receipts. For example, *mail@example.com*
Name or IP address of backup SMTP servers:	Enter fully qualified domain names or IP addresses. For example, *mail2.example.com* or *10.100.0.1*

Hostname and Networking



Hostname:	Enter a hostname you can use within your network to address the SonicWALL Email Security appliance. Enter a fully qualified domain name. For example, *emailsecurity.example.com*
Get all network settings from DHCP:	Select this if you want your SonicWALL Email Security appliance to get dynamic IP settings from the DHCP server on your network.
Use the static settings below:	Select this to assign your SonicWALL Email Security appliance a static IP address. Enter: • This machine's IP address • Primary DNS server IP address (the local DNS server that has the MX record for your mail server) • Fallback DNS server IP address • Default gateway IP address • Subnet mask

Date and Time

System Date and Time:	Select the current year, month, day, hour, and minute.
Current Time Zone:	Displays the currently configured time zone.
Available Time Zones:	Select the time zone for your area.
Automatically Adjust for Daylight Savings Time:	Select this if your area observes Daylight Saving Time.

Note: *To ensure optimal network performance of your SonicWALL Email Security appliance, it is important that you select the proper time zone.*

2. Click the **Apply Changes** button to save this configuration.
3. A popup will display. Click the **Continue** button to reboot the SonicWALL Email Security appliance with your new settings.
4. Disconnect the crossover cable from the SonicWALL Email Security appliance.
5. Reset your management computer's IP settings to work with your network. For example, if your network uses DHCP, reset your Local Area Connection to obtain an IP address and DNS settings dynamically from the server.
6. Reconnect your management computer to your network. You will use the network to access the SonicWALL Email Security appliance in the next steps.

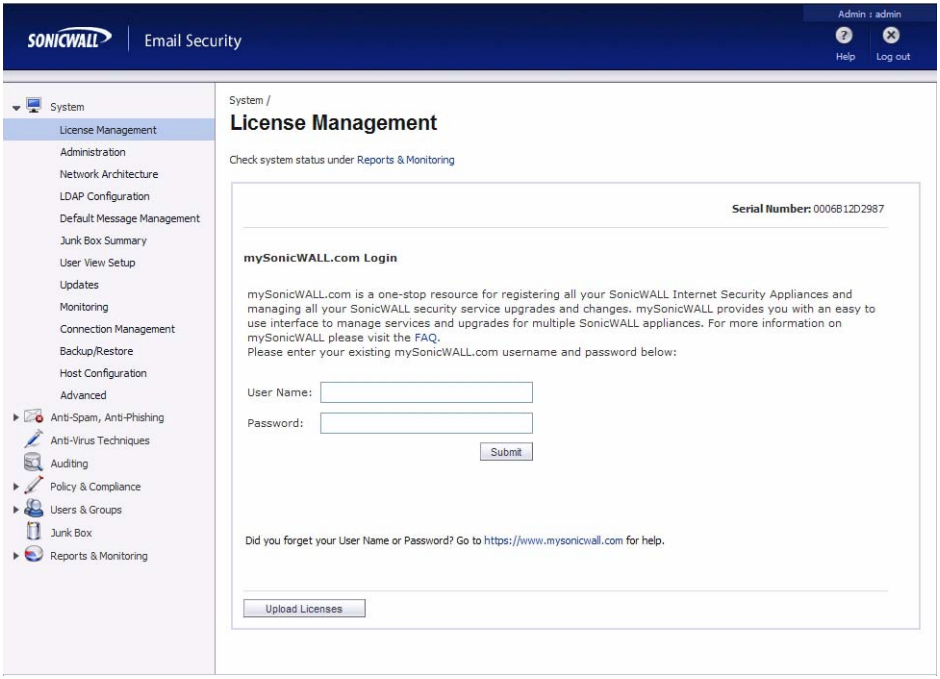
Activating the Email Security License Subscriptions

SonicWALL Email Security provides dynamic licensing, which allows you to activate your licenses by simply logging into your mysonicwall.com account. The mysonicwall.com server automatically uses the serial number and authentication code that came with your Email Security appliance.

Note: *If you purchased Total Secure Email, licensing is automatic and you do not need to take any action at all to activate your licenses.*

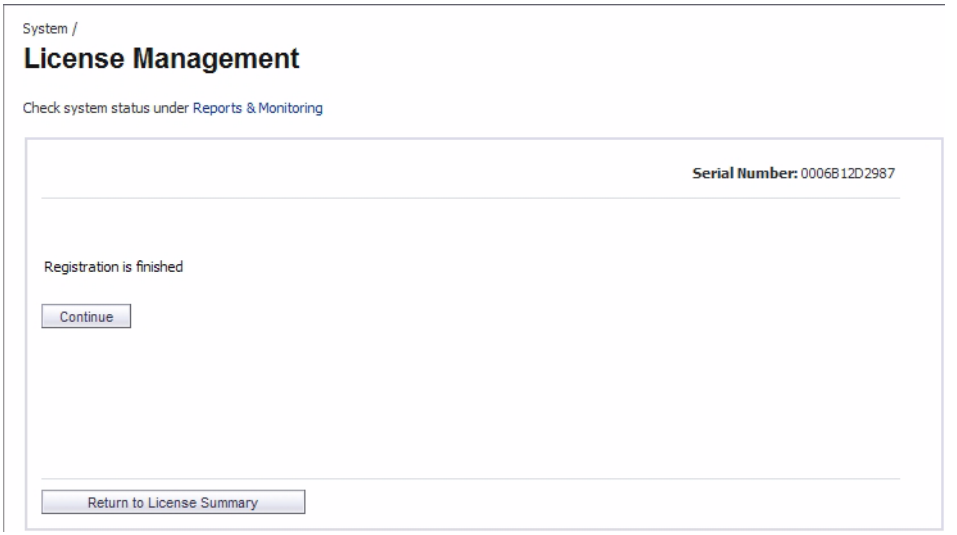
To activate Email Security license subscriptions:

1. Log in to the Email Security management interface.
2. In the System > License Management screen, type your mysonicwall.com **username** and **password** into the appropriate fields.

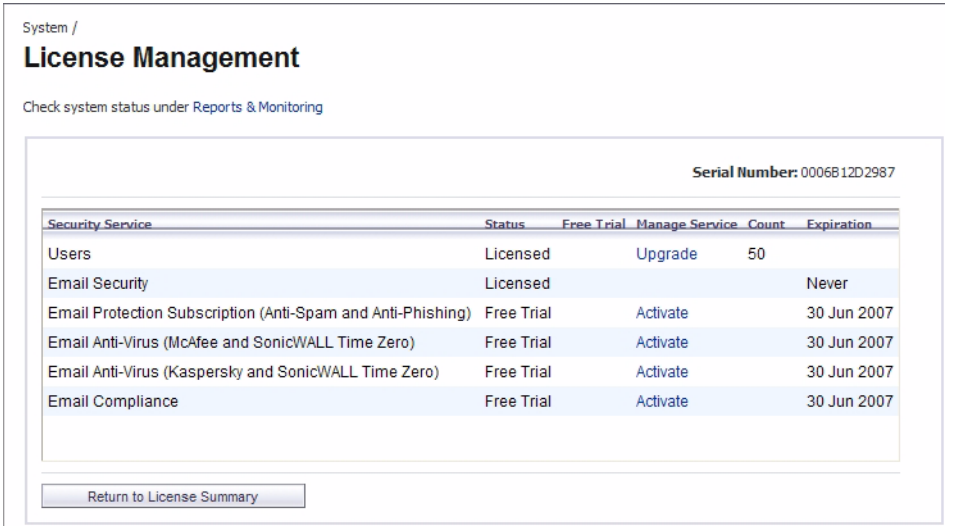


3. Click **Submit**.

4. In the next License Management screen, click **Continue**.



Licensing is now complete. The License Management screen displays the status, expiration date, and other information about your Email Security licenses.



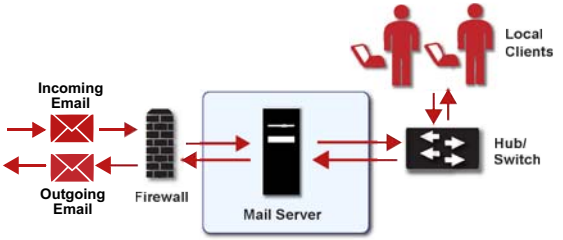
4 Connecting and Configuring Network Settings

This section contains the following sub-sections:

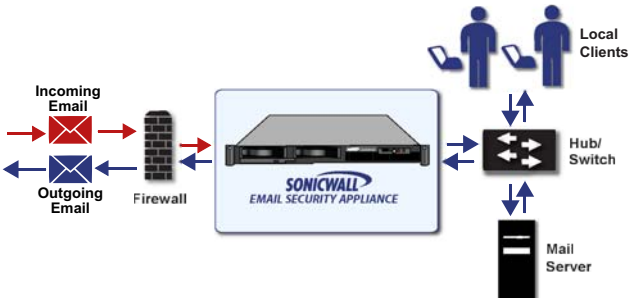
Connecting the SonicWALL Email Security Appliance to Your Network

Your SonicWALL Email Security appliance is designed to operate in most network setups with minimal configuration. The diagrams below provide a "before" and "after" view of a network using SonicWALL Email Security.

Mail Flow Before SonicWALL Email Security



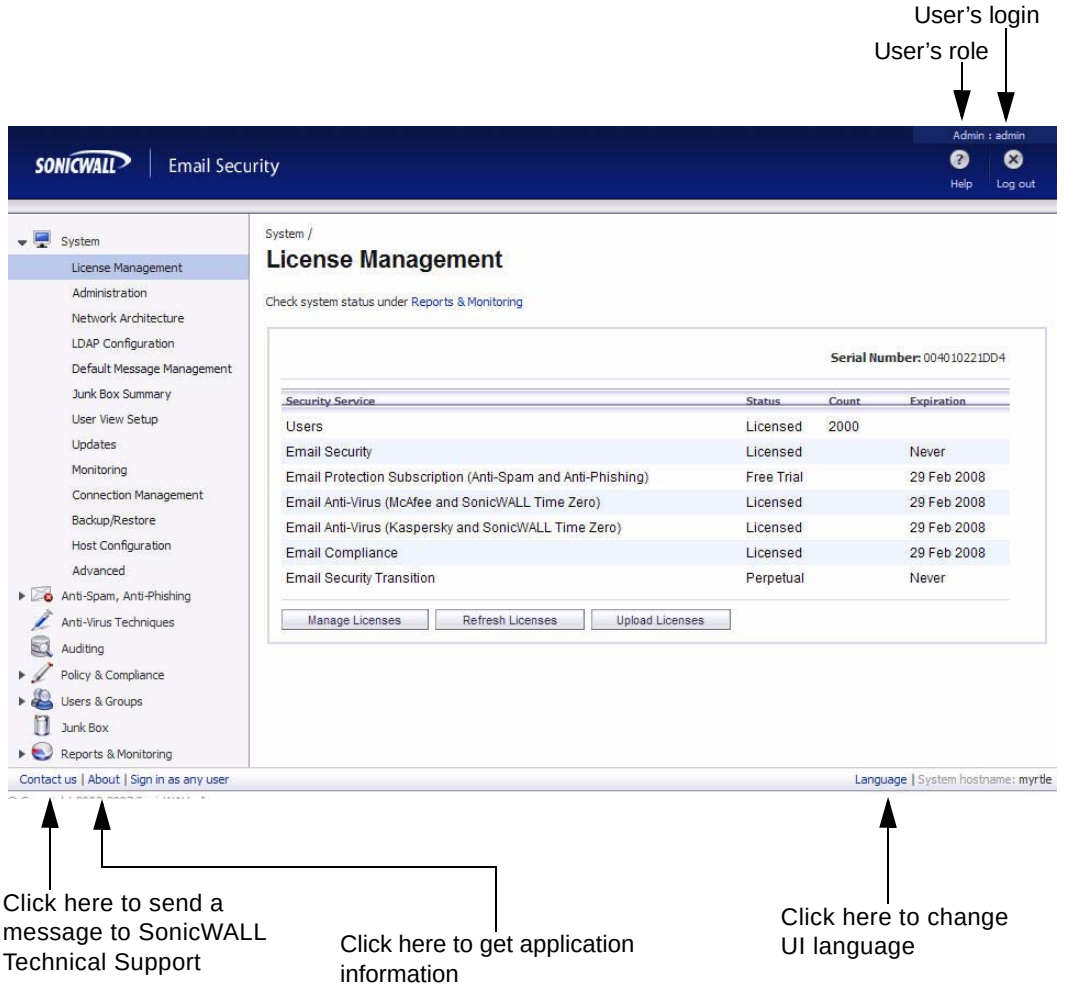
Mail Flow After SonicWALL Email Security



1. Plug one end of the provided Ethernet cable into the LAN port on the back of your SonicWALL Email Security appliance.
2. Plug the other end of the cable into an open port on your network hub or switch.

The SonicWALL Email Security Interface

This section describes how to navigate the SonicWALL Email Security Appliance user interface.



Change the Default Administrator Password

1. Login to the SonicWALL Email Security appliance using the IP address you entered in “Hostname and Networking” on page 13.
2. Enter a new management password into the **Password** field.
3. Navigate to the **System > Administration** page.
4. Enter it again in the **Confirm Password** field.
5. Click **Apply Changes**.

Using Quick Configuration to Set Up Email Management

The Quick Configuration page will walk you step-by-step through the configuration of your SonicWALL Email Security appliance. Use this window the first time you configure SonicWALL Email Security if you are installing SonicWALL Email Security as an All-In-One server and have only one downstream server.

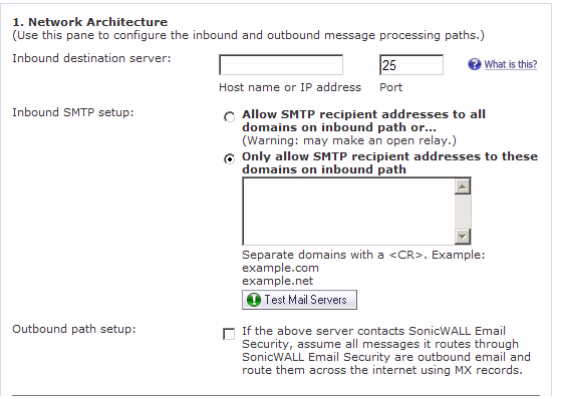
The information you enter for LDAP configuration is used to authenticate users as they log into their personal Junk Boxes.

Note: *For detailed configuration instructions, refer to the SonicWALL Email Security Administrator’s Guide.*

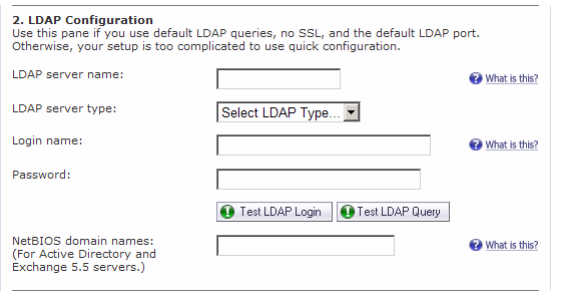
To use Quick Configuration:

1. Navigate to the **System > Administration** page.
2. Click **Click Here for Quick Configuration**.
3. In the Quick Configuration dialog box under **Network Architecture**, enter the host name or IP address and the port into the **Inbound destination server** fields.

The inbound destination server is the email server that will accept good email after SonicWALL Email Security removes and quarantines junk email. For example, this could be the IP address of a Microsoft Exchange server. The default port is 25.

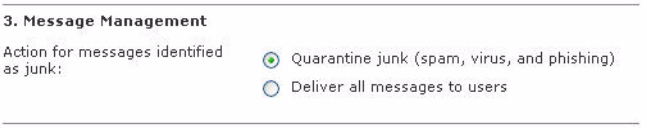


4. For Inbound SMTP setup, select one of the following:
   - **Allow SMTP recipient addresses to all domains on inbound path or...**
     This option does not restrict incoming email to any domain.
   - **Only allow SMTP recipient addresses to these domains on inbound path**
     This option allows you to specify the domains to which incoming email will be delivered. In the text box, type the allowed domains one per line.
5. Optionally click **Test Mail Servers** to verify connectivity to the downstream Email Security server specified in preceding steps.
6. Select the **Outbound path setup** check box to route outbound email across the Internet using MX records.
7. Under LDAP Configuration, enter a hostname or IP address into the **LDAP server name** field.
   This is often your Exchange server or email server.



8. Select the type of LDAP server from the **LDAP server type** drop-down list.

9. Enter a valid LDAP login name and password into the **Login name** and **Password** fields. Click **What is this?** for more information.
10. Click **Test LDAP Login** and **Test LDAP Query** to verify your settings.
11. Enter one or more NetBIOS domain name in the **NetBIOS domain names** field. Click **What is this?** for more information.
12. Under Message Management, specify how junk mail will be handled by selecting one of the following:
    - **Quarantine junk** - sends junk mail to the user's junk box
    - **Deliver all messages to users** - does not separate junk mail from good email



13. Under Junk Box Summary, to send daily summary messages about junk mail caught by SonicWALL Email Security, select **Send daily summaries**.

14. To allow users to preview their junk mail messages with unjunking them, select **Users can preview their own quarantined junk mail**.

    Summaries will contain a preview link for each junk email.
15. Type the URL where users can view their email junk boxes in the **URL for user view** field. Click **Test this Link** to verify connectivity.
16. Under Updates, click **Test Connectivity to SonicWALL** to test your connection to mysonicwall.com for automated software updates.

17. Click **Apply Changes**.

5 Verification and Further Configuration

This section contains the following subsections:

Routing Mail to Your SonicWALL Email Security Appliance

In order for your SonicWALL Email Security appliance to start filtering and monitoring mail, you must re-route mail traffic through your SonicWALL Email Security appliance. Mail traffic must pass from the Internet to the appliance, and then the appliance sends the good mail on to your mail server.

You have two choices to route mail traffic to your SonicWALL Email Security appliance instead of to your mail server:

- Change the MX record in your DNS server to resolve to the IP address of your SonicWALL Email Security appliance. You may have to work with your ISP to change this record.
- Create a rule in your firewall or router to route all port 25 (SMTP mail) traffic to your SonicWALL Email Security appliance. Refer to your firewall or router documentation for instructions on creating rules to route traffic.

Verifying Mail from the Internet Through Your SonicWALL Email Security Appliance

1. Go to an external mail account, for example Yahoo mail or GMail.
2. Create a new email message:

To:	An email address where you receive email that is on the mail server for which you have configured the SonicWALL Email Security appliance.
Subject:	SonicWALL Email Security Verification Message
Body:	SonicWALL Email Security Verification Message

3. Send the message.
4. In the SonicWALL Email Security appliance administrative interface, click the **Auditing** button on the top.
5. Check the **Inbound** auditing reports to make sure the email appears as Delivered.
6. Check the mail account you sent the message to. If you received the message, you have correctly configured your SonicWALL Email Security appliance.

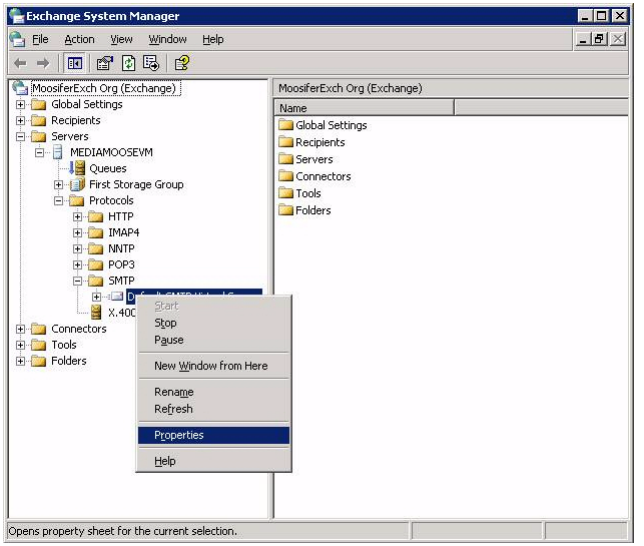
Configuring Outbound Mail Filtering

You can have your SonicWALL Email Security appliance filter outbound mail from your mail server to the Internet. To configure outbound mail filtering, you configure both your mail server and your SonicWALL Email Security appliance for the outbound mail path.

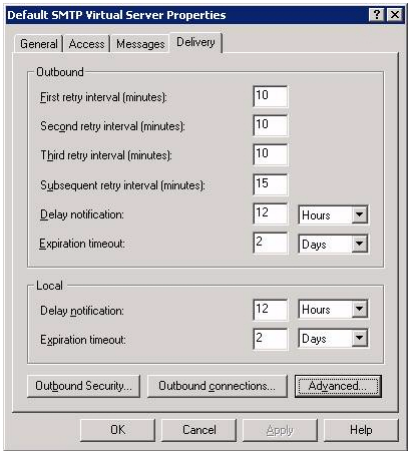
Configure the outbound mail destination of your mail server to point to the IP address or host name of your SonicWALL Email Security appliance. This is typically done by configuring a Smart Host on your mail server.

The configuration steps for Exchange Server 2003 are provided here. See the documentation on your mail server for specific instructions.

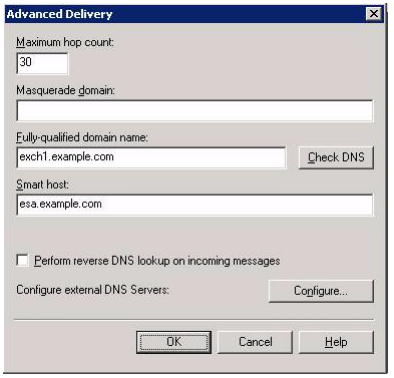
1. In the **Exchange System Manager**, navigate to **Servers > [servername] > Protocols > SMTP > Default SMTP Virtual Server** (or active server instance).
2. Right-click **Default SMTP Virtual Server**, and select **Properties**.



3. Browse to the **Delivery** tab, and click the **Advanced** button.



4. In the Smart Host field, enter the FQDN on your SonicWALL Email Security appliance (such as, esa.example.com). Note: The Exchange Server must be able to resolve this host name.



5. Click **OK**.

On your SonicWALL Email Security appliance, in the **Server Configuration > Network Architecture page**, configure a separate, outbound path to handle the outbound email flow at the appliance (if not already configured).

Configure the path to use the MTA (MX routing or SmartHost) under **Destination of Path**.

You need to configure something unique between the inbound and outbound path to distinguish inbound from outbound mail flow. A very simple way to do this is to have them listen on different ports or enter the IP address of the Exchange Server as the **Source IP Contacting Path** on the outbound path.

Example

Given this:

```
10.100.0.10: Exchange Server (exch1.example.com)
10.100.0.100: SonicWALL Email Security appliance (esa.example.com)
```

You might have two paths that look like this:

	Source IP	Listen On	Destination
Inbound	Any	Any:25	(proxy) exch1.example.com:25
Outbound	10.100.0.10	Any:25	MX

In this scenario, any message that arrives at the SonicWALL Email Security appliance from 10.100.0.10 will be treated as an outbound message, handed off to the MTA component in the system, which will deliver the message via MX-lookup on the domain in the **TO** field. Messages that arrive at the SonicWALL Email Security appliance from any other IP address will be treated as an Inbound message, and delivered directly to the Exchange server. The SonicWALL Email Security appliance always gives preference to specific matches (for example an exact IP address match takes precedence over “Any”).

Another example using port numbers to distinguish which path a message should take:

	Source IP	Listen On	Destination
Inbound	Any	Any:25	(proxy) exch1.example.com:25
Outbound	Any	Any:2525	MX

Another alternative would be to assign your SonicWALL Email Security appliance multiple IP addresses, and have it listen on one for inbound and one for outbound.

In all of the above cases, the admin will configure Exchange to deliver outbound email to the IP address and port number where the SonicWALL Email Security appliance is listening for outbound mail.

To test your SonicWALL Email Security appliance, click the **Auditing** button at the top of the SonicWALL Email Security appliance user interface and search for your sent email to verify it has been sent and received.

Troubleshooting

This section contains the following subsection:

- Configuring a Static IP Address

Configuring a Static IP Address

Complete the following section based on your operating system in order to configure your management computer with a static IP address:

Windows XP

1. From the **Start** menu, highlight **Connect To** and then select **Show All Connections.**
2. Open the **Local Area Connection Properties** window.
3. Double-click **Internet Protocol (TCP/IP)** to open the **Internet Protocol (TCP/IP) Properties** window.
4. Select **Use the following IP address** and type **192.168.168.50** in the **IP address** field.
5. Type **255.255.255.0** in the **Subnet Mask** field.
6. Click **OK** for the settings to take effect.

Windows 2000

1. From your Windows **Start** menu, select **Settings**.
2. Open **Network and Dial-up Connections**.
3. Click **Properties**.
4. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select **Use the following IP address** and type **192.168.168.50** in the **IP address** field.
6. Type **255.255.255.0** in the **Subnet Mask** field.
7. Click **OK** for the settings to take effect.

Windows NT

1. From the **Start** menu, highlight **Settings** and then select **Control Panel**.
2. Open **Network**.
3. Double-click **TCP/IP** in the **TCP/IP Properties** window.
4. Select **Specify an IP Address** and type **192.168.168.50** in the **IP address** field.
5. Type **255.255.255.0** in the **Subnet Mask** field.
6. Click **OK**, and then click **OK** again.
7. Restart the computer for the changes to take effect.

Regulatory Statement and Safety Instructions

Regulatory Model/Type	Product Name
1RK10-04D	Email Security 8000

This product hardware based on IBM xSeries 336 Type 8837, Model 15U. Refer to safety documentation in this manual and to the complete IBM Safety and EMC information on the SonicWALL Resource CD included with this product.

Additional language safety and EMC information can be found on the SonicWALL Resource CD included with this product.

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الأمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 Safety Information
（安全信息）。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας
(safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się
z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по
технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

Important:

All caution and danger statements in this documentation begin with a number. This number is used to cross reference an English caution or danger statement with translated versions of the caution or danger statement in the *IBM® Safety Information* book.

For example, if a caution statement begins with a number 1, translations for that caution statement appear in the *IBM Safety Information* book under statement 1.

Be sure to read all caution and danger statements in this documentation before performing the instructions. Read any additional safety information that comes with your server or optional device before you install the device.

Statement 1:

DANGER

Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect to properly wired outlets any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	To Disconnect:
1. Turn everything OFF.	1. Turn everything OFF.
2. First, attach all cables to devices.	2. First, remove power cords from outlet.
3. Attach signal cables to connectors.	3. Remove signal cables from connectors.
4. Attach power cords to outlet.	4. Remove all cables from devices.
5. Turn device ON.	

Statement 2:

CAUTION:
When replacing the lithium battery, use only IBM Part Number 33F8354 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

Do not:

- Throw or immerse into water
- Heat to more than 100°C (212°F)
- Repair or disassemble

Dispose of the battery as required by local ordinances or regulations.

Statement 3:

CAUTION:
When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.

DANGER

Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following.

Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.

CAUTION:
Never remove the cover on a power supply or any part that has the following label attached.

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

WARNING: Handling the cord on this product or cords associated with accessories sold with this product, will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

ADVERTENCIA: El contacto con el cable de este producto o con cables de accesorios que se venden junto con este producto, pueden exponerle al plomo, un elemento químico que en el estado de California de los Estados Unidos está considerado como un causante de cancer y de defectos congénitos, además de otros riesgos reproductivos. ***Lávese las manos después de usar el producto.***

For additional safety and regulatory information, refer to the IBM documentation located on the SonicWALL Resource CD included with this product.

Rack Installation Instructions

Review the documentation that comes with your rack cabinet for safety and cabling information. Before installing your server in a rack cabinet, review the following guidelines:

- Make sure that the room air temperature is below 35°C (95°F).
- Do not block any air vents; usually, 15 cm (6 in.) of air space in the rear and 5 cm (2 in.) in the front provides proper airflow.
- Plan the device installation starting at the bottom of the rack cabinet.
- Install the heaviest device in the bottom of the rack cabinet.
- Do not extend more than one device out of the rack cabinet at the same time.
- Remove the rack doors and side panels to provide easier access during installation.
- Connect the server to a properly grounded outlet.
- Do not overload the power outlet when installing multiple devices in the rack cabinet.
- The slide rails in this kit come preset to the correct length for installation in an IBM rack cabinet, and they are adjustable for other rack cabinets.
- The slide rails are marked (RIGHT/FRONT and LEFT/FRONT) for proper placement on the rack-cabinet flanges.

This symbol identifies a Caution statement. Always read the information that accompanies this symbol before you proceed with the installation.

Safety Information, Statement 4

Use safe practices when lifting.

≥18 kg (39.7 lb)

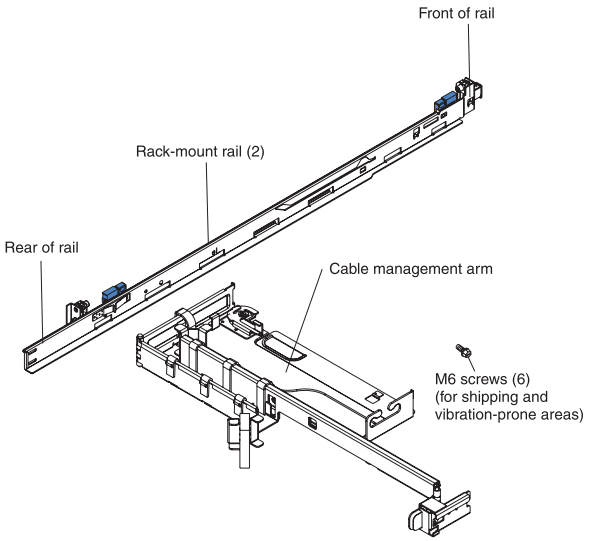
≥32 kg (70.5 lb)

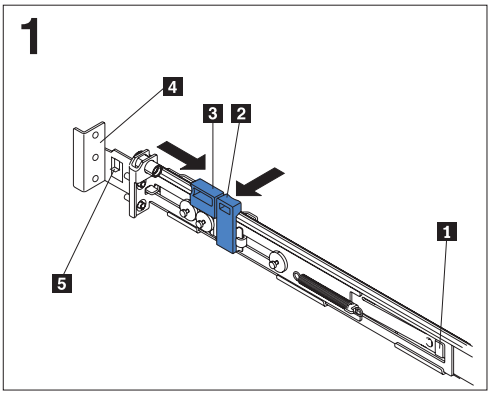
≥55 kg (121.2 lb)

Rack Safety Information, Statement 6

Do not place any objects on top of a rack-mounted device unless that rack-mounted device is intended for use as a shelf.

This server does not require any tools for the installation procedure unless you are shipping the server in the rack cabinet. If you are shipping the server in the rack cabinet, you need a Phillips screwdriver. The following illustration shows the items that you need for installing the server in a rack cabinet. If any items are missing or damaged, contact your place of purchase.

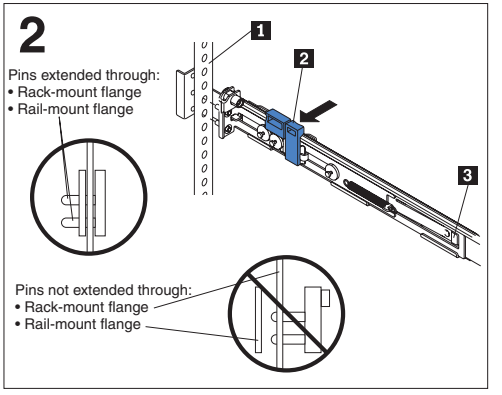




Slide the pins away from the rail-mount flange:

Press behind the slide-rail release latch 1 and hold it to prevent the rail from sliding back. Press the tab 2 away from the rail. Press the tab 3 back, and slide the rear rack-bracket pins away from the rail-mount flange 4 . Slide the pins back until the bracket stays in an open position.

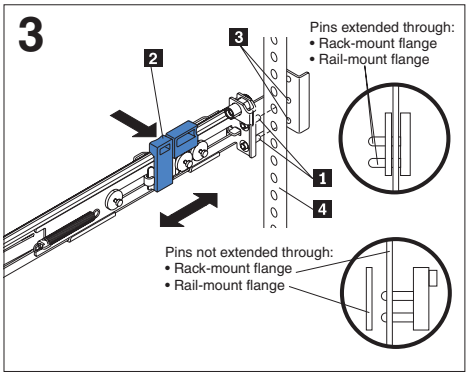
Attention: Do not remove tab 5 unless you are installing the rails on a non IBM rail-mount flange with a thickness greater than 3.175 mm (0.125 in.). If you remove tab 5 , you must insert an M6 screw through the bottom hole of the rail-mount flange 4 on all four flanges of the rack.



Attach the rear rail-adjustment bracket to the rack:

Place the rack-mount flange 1 between the rail-mount flange and the rack-bracket pins. Press the tab 2 ; the rack-bracket pins snap into place, sliding through the rack-mount flange 1 and rail-mount flange. Lift the slide-rail release latch 3 , and then slide the front rail toward the front of the rack.

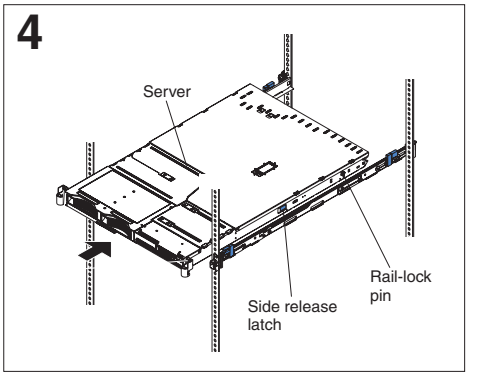
Attention: Make sure that the rail is securely clamped against the rack-mount flange.



Attach the front rail bracket to the rack:

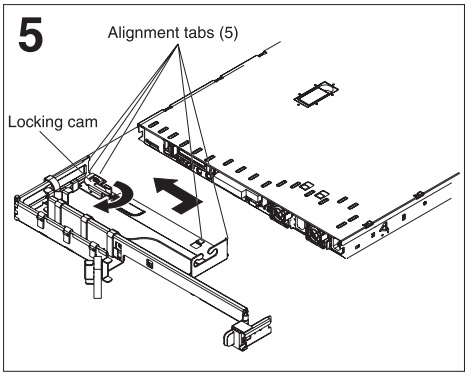
Press the tab 2 away from the rail. Slide the front rack-bracket pins 1 away from the rail-mount flange 3 until the front rail bracket stays open. Place the rack-mount flange 4 between the front rack-bracket pins 1 and the rail-mount flange 3 . Press the tab 2 away from the rail. The pins snap forward and extend through the rack-mount flange and the rail-mount flange.

Attention: Make sure that the rail is securely clamped against the rack-mount flange.



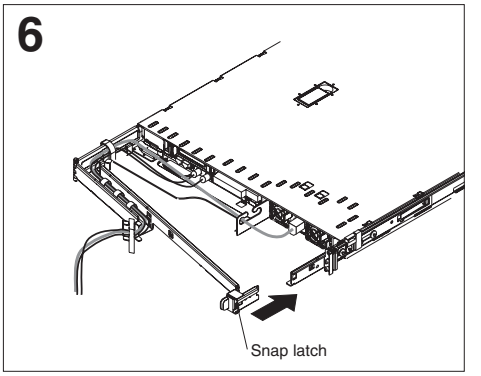
Insert the server into the rack cabinet:

Align the server on the slide rails and push the server into the rack cabinet. If the rail-lock pins are extended out, pull the side release latches toward you, which lifts up the rail-lock pins. Push the server into the rack the remainder of the way.



Install the cable-management arm:

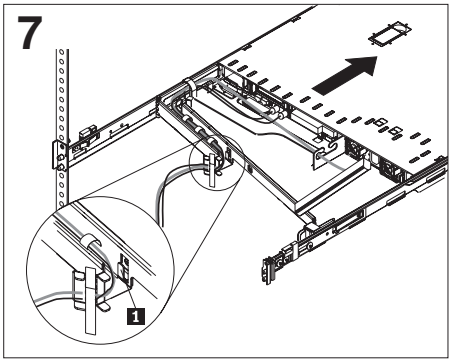
Insert the cable-management arm into the five slots in the rear of the server. When the cable-management arm is inside all five slots, slide the cable-management arm to the left by pulling the locking cam back, away from the server.

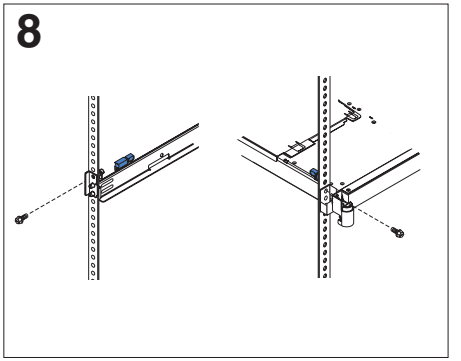


Connect the cables and secure the cable-management arm to the rack:

Pull the cable-management arm away from the server, and connect the cables to the server. Route the cables through the cable-management arm.

Move the cable-management arm toward the rail on the right side, and snap the latch onto the rail.





Extend the cable-management arm and fasten the cables:

Attention: Make sure that you route Fibre Channel cables through the tab **1** , to ensure proper bend radius and prevent damage to these cables.

Extend the cable-management arm by sliding the server toward the front of the rack. The rail-lock pins stop the server halfway along the rack. Secure the cables by using the straps that are attached to the cable-management arm.

Slide the server back into the rack cabinet.

Secure the server to the rack:

Before you transport the rack cabinet to another location with the server installed, you must secure the server to the rack. If necessary, disconnect the cables from the rear of the server; then, slide the server out of the rack 150 mm (6 in.) and insert the M6 screws in each slide rail. Then, secure the server to the rack cabinet with the M6 screws and reconnect the cables.

To remove the server from the rack, reverse these instructions. Store this information with your server documentation for future use.

First Edition (July 2004)

Printed in the U.S.A.

(1P) P/N: 25K9195

Copyright Notice

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Java is a trademark or registered trademark of Sun Microsystems, Inc. om the U.S. or other countries.

Apache Tomcat is a trademark of Apache Software Foundation.

Firebird is a registered trademark of the Firebird Foundation, Inc.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

SonicWALL GPL Source Code

GNU General Public License (GPL)

SonicWALL will provide a machine-readable copy of the GPL open source on a CD. To obtain a complete machine-readable copy, please send your written request, along with a certified check or money order in the amount of US $25.00 payable to “SonicWALL, Inc.” to:

General Public License Source Code Request

SonicWALL, Inc. Attn: Jennifer Anderson

1143 Borregas Ave.

Sunnyvale, CA 94089

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale CA 94089-1306
T +1 408.745.9600
F +1 408.745.9300
www.sonicwall.com

PN: 232-001160-00